Exhibit 86

ADVERTISEMENT

BUSINESS

U.S. election integrity depends on security-challenged firms

By FRANK BAJAK
ASSOCIATED PRESS | OCT 29, 2018

FEEDBACK

Early voters cast ballots Oct. 10, 2018, at the Lake County Government Center in Crown Point, Ind. Three companies sell and service more than 90 percent of the machines on which votes are cast and results tabulated. Experts say they skimp on security. (Joe Puchek/Post-Tribune)

It was the kind of security lapse that gives election officials nightmares. In 2017, a

SECTIONS

99¢ FOR 8 WEEKS
Offer ends 2/8

LOG IN

CORONAVIRUS IN ILLINOIS UPDATES

Later, at a tense hearing, Chicago's Board of Elections dressed down the top three executives of Election Systems & Software, the nation's dominant supplier of election equipment and services.

ADVERTISEMENT

FEEDBACK

Advertisement

The three shifted uneasily on folding chairs as board members grilled them about what went wrong. ES&S CEO Tom Burt apologized and repeatedly stressed that there was no evidence hackers downloaded the data.

The Chicago lapse provided a rare moment of public accountability for the closely held businesses that have come to serve as front-line guardians of U.S. election security.

A trio of companies — ES&S of Omaha, Neb.; Dominion Voting Systems of Denver and Hart InterCivic of Austin, Texas — sell and service more than 90 percent of the machinery on which votes are cast and results tabulated. Experts say they have long skimped on security in favor of convenience, making it more difficult to detect intrusions such as occurred in Russia's 2016 election meddling.

[Most read] Wisconsin prosecutors seek new arrest warrant for Kyle Rittenhouse, higher bond »

FEEDBACK

The businesses also face no significant federal oversight and operate under a shroud of financial and operational secrecy despite their pivotal role underpinning American democracy.

Advertisement

In much of the nation, especially where tech expertise and budgets are thin, the companies effectively run elections either directly or through subcontractors.

"They cobble things together as well as they can," University of Connecticut election-technology expert Alexander Schwartzman said of the industry leaders. Building truly secure systems would likely make them unprofitable, he said.

The costs of inadequate security can be high. Left unmentioned at the Chicago hearing: The exposed data cache included roughly a dozen **encrypted passwords for ES&S employee accounts**. In a worst-case scenario, a sophisticated attacker could have used them to infiltrate company systems, said Chris Vickery of the security firm Upgard, which discovered the data lapse.

"This is the type of stuff that leads to a complete compromise," he said. ES&S said the passwords were only used to access the company's Amazon cloud account and that "there was no unauthorized access to any data or systems at any time."

FEEDBACK

[Most read] Worst cold snap in 2 years to freeze Chicago over weekend after cold front moves in starting Thursday night »

All three of the top vendors declined to discuss their finances and insist that security concerns are overblown. ES&S, for instance, said in an email that "any assertions about resistance to input on security are simply untrue" and argued that for decades the company has "been successful in protecting the voting process."

Stonewalling on security

Many voting systems in use today across the more than 10,000 U.S. election jurisdictions are prone to security problems. Academic computer scientists began hacking them with ease more than a decade ago, and not much has changed.

Hackers could theoretically wreak havoc at multiple stages of the election process. They could alter or erase lists of registered voters to sow confusion, secretly introduce software to flip votes, scramble tabulation systems or knock results-reporting sites offline.

There's no evidence any of this has happened, at least not yet.

The vendors say there's no indication hackers have penetrated any of their systems. But authorities acknowledge that some election mischief or malware booby traps may have gone unnoticed.

[Most read] What you need to know about the COVID-19 vaccine second dose: timely appointments, adequate supplies, knowledge of side effects »

On July 13, U.S. special counsel Robert Mueller **indicted 12 Russian military intelligence operatives** for, among other things, infiltrating state and local election systems. Senior U.S. intelligence officials say the Kremlin is well-positioned to rattle confidence in the integrity of elections during this year's midterms, should it choose to.

FEEDBACK

ADVERTISEMENT

Election vendors have long resisted open-ended vulnerability testing by independent, ethical hackers — a process that aims to identify weaknesses an adversary could exploit. Such testing is now standard for the Pentagon and major banks.

While the top vendors claim to have stepped up their cybersecurity game, experts are skeptical.

"The industry continues to stonewall the problem," said Bruce McConnell, a Department of Homeland cybersecurity czar during the Obama administration. Election-vendor executives routinely issue assurances, he said, but don't encourage outsiders to inspect their code or offer "bug bounties" to researchers to seek out flaws in their software.

Sen. Ron Wyden, an Oregon Democrat, has long criticized what he calls the industry's "severe underinvestment in cybersecurity." At a July hearing, he accused the companies of "ducking, bobbing and weaving" on a series of basic security questions he'd asked them.

[Most read] Coronavirus in Illinois updates: State redirects 97,000 unused doses from federal program; new daily vaccination record set as 3,314 new COVID-19 cases and 69 more deaths reported »

FEEDBACK

ES&S told The Associated Press that it allows independent, open-ended testing of its corporate systems as well as its products. But the company would not name the testers and declined to provide documentation of the testing or its results.

Dominion's vice president of government affairs, Kay Stimson, said her company has also had independent third parties probe its systems but would not name them or share details. Hart InterCivic, the No. 3 vendor, said it has done the same using the Canadian cybersecurity firm Bulletproof, but would not discuss the results.

ES&S hired its **first chief information security officer** in April. None of the big three vendors would say how many cybersecurity experts they employ. Stimson said that "employee confidentiality and security protections outweigh any potential disclosure."

Sloppy software and vulnerability

Experts say they might take the industry's security assurances more seriously if not for the abundant evidence of sloppy software development, a major source of vulnerabilities.

During this year's primary elections, ES&S technology failed on several fronts.

[Most read] Illinois redirects 97,000 vaccine doses from federal nursing home program Pritzker has criticized for moving too slowly »

In Los Angeles County, more than 118,000 names were left off printed voter rolls. A subsequent outside audit blamed **sloppy system integration** by an ES&S subsidiary during a database merge.

No such audit was done in Kansas' most populous county after a **different sort of error** in newly installed ES&S systems delayed the vote count by 13 hours as data uploading from thumb drives crawled.

FEEDBACK

University of Iowa computer scientist Douglas Jones said both incidents reveal mediocre programming and insufficient pre-election testing. And voting equipment vendors have never seemed security conscious "in any phase of their design," he said.

For instance, industry leader ES&S sells vote-tabulation systems equipped with cellular modems, a feature that experts say sophisticated hackers could exploit to tamper with vote counts. A few states ban such wireless connections; in Alabama, the state had to force ES&S to remove them from machines in January.

ADVERTISEMENT

"It seemed like there was a lot more emphasis about how cool the machines could be than there was actual evidence that they were secure," said John Bennett, the Alabama secretary of state's deputy chief of staff.

[Most read] Third stimulus check updates: Biden shows flexibility but tells House to ‘go big’ on COVID-19 relief package »

ADVERTISEMENT

FEEDBACK

California conducts some of the most rigorous scrutiny of voting systems in the U.S. and has repeatedly found chronic problems with the most popular voting systems. Last year, a state security contractor found **multiple vulnerabilities in ES&S's Electionware system**that could, for instance, allow an intruder to erase all recorded votes at the close of voting.

In 2014, the same contractor, Jacob Stauffer of the security firm Coherent Cyber, found "multiple critical vulnerabilities" in Dominion's Democracy Suite that could allow skilled hackers to compromise an election's outcome.

"These systems are Frankenstein's monster, essentially," Stauffer said.

The federal Department of Homeland Security began offering confidential vulnerability testing to vendors over the summer. But only one vendor has submitted to such testing, said an agency official who spoke on condition of anonymity because the official was not authorized to discuss the matter publicly.

Stalled innovation

More competition might help, but industry barriers to smaller vendors are "absolutely enormous," said Larry Moore, president of upstart Clear Ballot. Its auditable voting system took two and a half years to **win federal certification** at a cost of $1 million.

FEEDBACK

[Most read] Chicago Bears Q&A: What could the trade compensation for Deshaun Watson look like? Is Mitch Trubisky still the best option at QB in 2021? Would Alabama's Mac Jones be a reach with the No. 20 pick? »

Startups are hard-pressed to disrupt an industry whose main players rely heavily on proprietary technologies. ES&S and other vendors have jealously guarded them in court — and also unleash lawyers against election officials who purchase competitors' products.

In October, ES&S sued Cook County, seeking to void its $30 million, 10-year contract with a competitor. It also recently threatened Louisiana and Douglas County, Kansas, with lawsuits for choosing other suppliers.

Cook County elections director Noah Praetz said litigious behavior only chills modernization. Competition and innovation are already hampered in an industry

with "really low" margins, especially considering limited government funding for election equipment.

"The market isn't functioning real well," he said.

Limited oversight

Elections are run by the states, whose oversight of suppliers varies. California, New York and Colorado are among states that keep a close eye on the vendors, but many others have cozier relationships with them.

[Most read] How a fight over slot machines led state investigators to probe two Illinois video gambling kings »

And the vendors can be recalcitrant. In 2017, for instance, Hart InterCivic refused to provide Virginia with a paperless e-Slate touchscreen voting machine for testing, said Edgardo Cortes, then the state election commissioner.

FEEDBACK

In this year's midterms — as in the 2016 election — roughly 1 in 5 voters will use such electronic machines. Their tallies cannot be verified because they produce no paper record.

Cortes decided to decertify all such systems. If anyone tried to break in and alter votes, he concluded, "there was really no way for us to tell if that had happened." Hart InterCivic's vice president of operations, Peter Lichtenheld, did not dispute Cortes' account in July Senate testimony, but said its Virginia customers were already moving to newer machines.

At the federal level, no authority accredits election vendors or vets them or their subcontractors. No federal law requires them to report security breaches or to perform background checks on employees or subcontractors.

Election vendors don't even have to be U.S. companies. Dominion was Canadian-owned until July, when a New York private equity firm bought a controlling interest.

Federal oversight is limited to the little-known Election Assistance Commission, a 30-employee agency that certifies voting equipment but whose recommendations are strictly voluntary. It has no oversight power and cannot sanction manufacturers for any shortcomings.

"We can't regulate," EAC chairman Thomas Hicks said during a July 11 congressional hearing when the question came up. Neither can DHS, even though it designated the nation's election systems "critical infrastructure" in early 2017.

Topics: Elections, Russia, Ron Wyden

Getting this Treasure is impossible! Prove us wrong

HERO WARS | SPONSORED

If You Like to Play, this City-Building Game is a Must-Have. Do Install.

RGE OF EMPIRES | SPONSORED

Most Beautiful Beach Cities Where You Can Live for Cheap

THRILLIST | SPONSORED

Why These Credit Cards Are Ideal For College Students

Every State's Top High School Football Stadium

NERDWALLET | SPONSORED

CHICAGO TRIBUNE

Fox News stars Sean Hannity, Tucker Carlson and fired anchor Ed Henry named in sexual harassment lawsuit

CHICAGO TRIBUNE

MSNBC anchor Stephanie Ruhle 'sick and scared' after she, husband and kids tested positive for COVID

By **DAVID BAUDER**

SUN SENTINEL

A 'healthy' doctor died two weeks after getting a COVID-19

vaccine

50 Best Songs of All Time, Ranked by Rolling Stone

BIG EDITION | SPONSORED

Head-Turning 2021 Cars Loaded Beyond Belief

LUXURY SUVS | SEARCH ADS | SPONSORED

CHICAGO TRIBUNE

Column: Chief Justice John Roberts, please do America a favor and make Donald Trump go away

CHICAGO TRIBUNE

Judge gives Balfour 3 life sentences, calls his soul 'barren'

By JASON MEISNER AND STACEY ST. CLAIR

You May Like

Sponsored Links by Taboola

Colorado Launches New Guidelines For Cars Used Less Than 50 Miles/Day

BindRight Auto Insurance Quotes

FEEDBACK

ost Scenic Drive in All 50 States

illist

Worst Glovemen at Every Position in MLB History

Stadium Talk

This Is Where the Majority of Singles Over 50 Are Finding Love in Denver

SilverSingles

ADVERTISEMENT

CASE 0:22-cv-00098-JMB-JFD Doc. 1-87 Filed 01/18/22 Page 13 of 14

CONNECT

TRIBUNE PUBLISHING

New York Daily News
The Baltimore Sun
Orlando Sentinel
Sun Sentinel of Fla.
The Morning Call of Pa.
Hartford Courant
Daily Press of Va.
The Virginian-Pilot
The Daily Meal
Studio 1847

COMPANY INFO

Careers
About us
Help Center
Privacy Policy
Terms of Service
Archives
Contact us
Coupons
Local print ads
Manage Web Notifications
Chicago Tribune Store
Media kit

Copyright © 2021, Chicago Tribune